[Separate counsel for each defendant joining this joint brief are listed on the signature page]

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN JOSE DIVISION**

WINSTON SMITH; JANE DOE I; and JANE DOE II, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

FACEBOOK, INC.; AMERICAN CANCER SOCIETY, INC.; AMERICAN SOCIETY OF CLINICAL ONCOLOGY, INC.; MELANOMA RESEARCH FOUNDATION; ADVENTIST HEALTH SYSTEM; BJC HEALTHCARE; CLEVELAND CLINIC; and UNIVERSITY OF TEXAS—MD ANDERSON CANCER CENTER,

Defendants.

Case No. 5:16-cv-01282-EJD

**DEFENDANTS' JOINT REPLY IN SUPPORT OF THEIR MOTION TO DISMISS THE COMPLAINT**

Date: November 17, 2016
Time: 9:00 a.m.
Dept.: 4, 5th Floor
Before: Hon. Edward J. Davila

**TABLE OF CONTENTS**

## TABLE OF AUTHORITIES

**Cases**

**Statutes**

**Regulations**



**Other Authorities**

## PRELIMINARY STATEMENT

Plaintiffs' hyperbole aside, this is a case about the routine transmission and receipt of data that does not identify any individual person or convey any sensitive health information. Defendants' opening brief identified three overarching, independent reasons why the complaint should be dismissed: (1) plaintiffs have not alleged any concrete harm and thus lack standing; (2) plaintiffs affirmatively consented to the data collection that they claim took place; and (3) the complaint establishes that each defendant was a party to all relevant communications and therefore did not "wiretap" anyone. Defendants further demonstrated that this Court lacks personal jurisdiction over the healthcare defendants, and that plaintiffs expressly declined to allege that any of the healthcare defendants acted with intent. Plaintiffs barely respond.

First, plaintiffs have all but abandoned their "economic damage" theory of standing, apparently recognizing that they cannot claim "that the value of their information was somehow diminished" by defendants' alleged conduct. *Facebook Internet*, 140 F. Supp. 3d at 931-32. Plaintiffs instead shift their focus to the bare contention that defendants violated some unspecified "right to privacy" in plaintiffs' "medical information." But plaintiffs do not explain how defendants caused *harm* to their privacy interests, let alone the *concrete* harm necessary for standing. Nor have they shown that the simple transmission and receipt of data has ever supported a federal lawsuit—all authority is to the contrary.

Second, plaintiffs quibble with portions of the healthcare defendants' disclosures while *ignoring* the disclosures most relevant to their claims: Facebook's Data Policy and Cookie Policy. These documents state that, unless they opt out, Facebook will receive information about its users' visits to certain websites "across the Internet and mobile ecosystem" that use Facebook features, and will use such information to help show ads. Instead of addressing these policies, plaintiffs contend that they could assent to them only under the conditions imposed by HIPAA—a statute that applies only to an enumerated set of transactions (not visits to public websites); protects only "medical information" that can "identify" an individual (not generic, public URLs); provides no private right of action (and cannot be channeled through separate claims); and applies only to covered entities (which Facebook, ACS, ASCO, and MRF concededly are not).

Third, plaintiffs openly acknowledge that the communications their browsers sent to the healthcare defendants were *separate* from those they sent to Facebook—and they do not contend that any party interfered in any way with communications sent to another party. Under well-established Circuit precedent, this means that plaintiffs have not been wiretapped. Ignoring that precedent, plaintiffs double down on the allegation that they had no reason to know that their browsers were sending the separate communications to Facebook. But even if that were true (and the complaint's own allegations prove otherwise), it could not save their wiretapping claim.

Plaintiffs' brief also confirms the additional flaws in their claims against the healthcare defendants. Incredibly, they argue that any company that even *communicates* with a California-based Internet service is subject to jurisdiction in this State, regardless of whether the action was knowing or even directed to California. And plaintiffs still profess no knowledge as to whether the healthcare defendants have done anything willfully, while continuing to assert claims against them that specifically require intent.

Tellingly, plaintiffs barely mention this Court's decision in *Facebook Internet*—even though it is dispositive of each of their claims. The complaint should be dismissed.

## ARGUMENT[1]

### I. THE COMPLAINT SHOULD BE DISMISSED UNDER RULE 12(b)(1) BECAUSE THIS COURT LACKS SUBJECT MATTER JURISDICTION.

Defendants argued that in light of *Spokeo*, plaintiffs cannot rely on the theory of pure "statutory" standing that saved three of the claims in *Facebook Internet* (DB 10-11), and that their failure to allege a concrete injury dooms *all* of their claims, both statutory and common-law (DB 11-13).[2] Plaintiffs do not dispute the first point, but argue that they have alleged two forms of concrete injury that are sufficient to establish standing. PB 9-11. First, they argue that an intangible "privacy harm" supports standing on the Wiretap Act and CIPA claims, but not on the

[1] "DB" refers to defendants' brief in support of their motion to dismiss. "PB" is plaintiffs' opposition brief. Short-form citations are used for cases cited in the opening brief.

[2] Defendants also contended that plaintiffs failed to allege a "particularized" harm against BJC and Cleveland Clinic. DB 13 n.6. Plaintiffs provide no response other than a conclusory assertion: "Plaintiffs plead 'particularized' injury." PB 9 n.16.

other eight other claims that they assert. *See* PB 9-11 (arguing repeatedly and exclusively that their alleged "privacy harm" arises from "rights granted by statute" and "statutory violation[s]"). Second, plaintiffs assert a tangible "economic harm" as a basis for standing on all of their statutory and common law claims. PB 11. Both theories fail.

**A. Plaintiffs Have Not Alleged a Concrete "Privacy Harm."**

In *Spokeo*, the Supreme Court held that "Article III standing requires a concrete injury even in the context of a statutory violation," but reaffirmed precedents holding that certain "intangible *injuries*" can qualify as concrete harms for purposes of standing. 136 S. Ct. at 1549 (emphasis added). The Court explained that in determining whether an intangible injury that gives rise to a statutory claim "constitutes injury in fact, both history and the judgment of Congress play important roles." *Id.* Accordingly, it instructed reviewing courts to consider (1) whether the "alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts"; and (2) whether the legislature has made a "judgment" to "elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." *Id.* (alteration omitted). Because plaintiffs have failed to allege *any* intangible harm, the Court need not even reach this test. But both factors nevertheless confirm that plaintiffs lack standing.

**1. Plaintiffs Have Not Sufficiently Alleged—or Even Meaningfully Described—Any "Privacy Harms" They Have Suffered.**

Plaintiffs' brief assumes that they have suffered an "intangible harm" to their "privacy" rights. PB 9. That is wholly insufficient. Even "at the pleading stage," a plaintiff is required to "*clearly* . . . allege facts demonstrating each element" of standing, including its injury-in-fact requirement. *Spokeo*, 136 S. Ct. at 1547 (emphasis added); *see also City of S. Lake Tahoe v. Cal. Tahoe Reg'l Planning Agency*, 625 F.2d 231, 237 n.7 (9th Cir. 1980). And it is well established that "'rights' are not a type of injury by itself, and an allegation that a defendant violated a [right] is not sufficient to confer standing; the plaintiff must also allege that she has been *injured* by the violation." *Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 882 (N.D. Ill. 2014) (emphasis added). Plaintiffs' complaint broadly accuses defendants of "violation[s] of their

privacy rights" and baldly asserts that "what the Plaintiffs intended to remain private is no longer so" (Compl. ¶¶ 3, 347), but it does not articulate any *harm*—emotional, physical, or otherwise—flowing from these claimed privacy violations. That is likely because (1) plaintiffs did not suffer any such harm and/or (2) they understand that such allegations would create a sea of individualized issues, rendering class certification impossible. Either way, plaintiffs' vague incantations of "privacy rights" are nothing more than restatements of their claims that the statutes were violated. That is manifestly insufficient after *Spokeo*. *See* 136 S. Ct. at 1549.

**2. Plaintiffs' Claims Bear No Relationship to Claims that Have Traditionally Been Regarded as Providing a Basis for Suit.**

Even if plaintiffs had alleged an intangible "privacy harm," it would not resemble the kind "that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Spokeo*, 136 S. Ct. at 1549. The right of privacy was not recognized in *any* form during the relevant period: "immediately before and after the framing of the Constitution." *Vermont Agency of Natural Res. v. U.S. ex rel. Stevens*, 529 U.S. 765, 774-76 (2000); *see Spokeo*, 136 S. Ct. at 1549 (relying on *Vermont Agency* in discussing the importance of "historical practice"); RESTATEMENT (SECOND) OF TORTS § 652A cmt. a. ("Prior to 1890 no English or American court had ever expressly recognized the existence of the right [to privacy]."). As first recognized, the right to privacy was narrowly limited to conduct that would result in "mental pain and distress[] far greater than could be inflicted by mere bodily injury," Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195-96 (1890)—a far cry from the transmission of URLs in the context of routine internet surfing.

Even under *today*'s law, plaintiffs' alleged injuries do not bear a close relationship to claims that would support a privacy suit. Courts routinely reject "data privacy claims similar to the ones brought by Plaintiffs." *Facebook Internet*, 140 F. Supp. 3d at 930. That is because "nothing in the precedent of the Ninth Circuit or other appellate courts confers standing . . . based on nothing more than the unauthorized disclosure of personal information." *In re Google*,

*Inc. Privacy Policy Litig.*, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28, 2012).[3] Plaintiffs cite a hodgepodge of cases permitting certain *other* types of privacy claims to proceed—a challenge to a law banning the use of contraceptives, *see Griswold v. Connecticut*, 381 U.S. 479, 485-86 (1965), and the nonconsensual practice of physically testing government employees to obtain "highly private and sensitive medical genetic information," *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1264 (9th Cir. 1998). But the URLs at issue here are not "sensitive medical information"—they are static links to public web pages. They reveal no one's diagnosis or medical condition; they merely indicate that someone—perhaps a doctor, student, or researcher—visited a website for some unknown purpose. Plaintiffs do not (and cannot) contend that a suit based on the routine practices at issue here has ever been permitted to proceed. The post-*Spokeo* cases they cite (PB 10-11) involved fundamentally different conduct.[4]

**3. Plaintiffs Have Not Shown a Legislative Intent To Create Standing.**

Plaintiffs also have not shown that Congress or the California legislature intended to establish standing based on a bare violation of the Wiretap Act or CIPA. They point to nothing at all in CIPA's legislative history. As for the Wiretap Act, plaintiffs rely on a single quotation from a subcommittee report on the ECPA stating that "Congress must act to protect the privacy

[3] *See, e.g.*, *Low*, 2011 WL 5509848, at *1, *6 (plaintiff "failed to put forth a coherent theory of how his personal information was disclosed or transferred to third parties, and how it ha[d] harmed him"); *iPhone*, 2011 WL 4403963, at *1, 4 (no standing for violations of "privacy rights" because plaintiffs "d[id] not identify what harm (if any) resulted from the access or tracking of their personal information"); *LaCourt*, 2011 WL 1661532, at *3-6 (no harm caused by defendant's use of plaintiffs' personal information for targeted advertising); *Zappos.com*, 108 F. Supp. 3d at 951, 962 n.5 (no showing that loss of privacy "amount[ed] to a concrete and particularized injury"); *see also Khan*, 2016 WL 2946165, at *1, *6 (no standing for privacy loss in data breach where plaintiff did not identify "potential damages arising from such a loss").

[4] *See Bona Fide Conglomerate v. SourceAmerica*, 2016 WL 3543699, at *8 (S.D. Cal. June 29, 2016) (standing for CIPA claim where defendants "secretly recorded" conversations of plaintiff's employees "to obtain confidential and privileged [ ] information to use against [plaintiff]," who spent "significant resources to respond"); *Nickelodeon*, 2016 WL 3513782, at *6-8 (standing based on alleged disclosure of minors' private, personal information in the face of defendant's express assurances that it would neither collect nor disclose that information); *Mey v. Got Warranty, Inc.*, 2016 WL 3645195, at *1 (N.D. W. Va. June 30, 2016) (standing for TCPA claim: "unwanted calls cause direct, concrete, monetary injury by depleting limited minutes," "deplet[ing] a cell phone's battery," and "wasting the consumer's time").

of our citizens," and that "[i]f we do not, we will promote the gradual erosion of this precious right." PB 11 (quoting S. Rep. No. 99-541, at 5 (1986)). This generalized language falls far short of the mark. In enacting the Fair Credit Reporting Act—the federal statute at issue in *Spokeo*—Congress found that "[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with . . . respect for the consumer's *right to privacy*." 15 U.S.C. § 1681(a)(4) (emphasis added). *Spokeo* found this insufficient to evince intent to expand the class of people who may sue in federal court: "Article III standing requires a concrete injury even in the context of a statutory violation. . . . . A violation of one of the FCRA's procedural requirements may result in no [concrete] harm" and thus no standing. 136 S. Ct. at 1549-50.

**B. Plaintiffs Have Not Alleged a Concrete "Economic Harm."**

Plaintiffs devote only a single paragraph to their economic theory of harm, asserting that they "allege[d] a robust market for the sensitive medical information wrongfully disclosed and tracked," and that "[t]his is enough." PB 11. Not so: Even assuming "that the information collected . . . ha[d] economic value," plaintiffs have no standing because they did not allege that the "purported conduct lessened the value of that information or affected its marketability." *Facebook Internet*, 140 F. Supp. 3d at 930-31; *see* DB 11-13 & n.5 (collecting cases).

Plaintiffs' sole authority—*In re Anthem, Inc. Data Breach Litigation*, 2016 WL 3029783 (N.D. Cal. May 27, 2016)—does not support their argument. *Anthem* did not address standing. And it merely held that the plaintiffs did not have to prove that the defendants had "*usurp[ed]* their ability to sell" their personally-identifiable information. *Id.* at *15 (emphasis added). Defendants do not seek to impose that burden here; under *Facebook Internet*, plaintiffs simply had to allege that the value of their information was *diminished* as a result of defendants' alleged conduct, and explain how. The *Anthem* plaintiffs made that showing by alleging that because of a data breach, criminals could "empty [their] bank account[s]" and "commit various types of fraud." *Id.* The court found that these allegations "could be read to infer that . . . the value of Plaintiffs' [information] decreased as a result of the Anthem data breach." *Id.* Plaintiffs have not made that claim, because mere data *collection* does not create the risks of theft and fraud resulting from a data *breach* that exposes someone's information to unauthorized third parties.

Because plaintiffs lack standing, the complaint should be dismissed as to all defendants.

## II. THE CLAIMS AGAINST THE HEALTHCARE DEFENDANTS SHOULD BE DISMISSED UNDER RULE 12(b)(2).

### A. The Court Lacks Personal Jurisdiction over the Healthcare Defendants.

Plaintiffs argue that the Court may exercise both general and specific jurisdiction over the healthcare defendants because they allegedly installed Facebook's code on their websites and because Facebook has its headquarters in California. PB 12; Compl. ¶¶ 265, 278. This argument runs counter to well-established and controlling law.

The Supreme Court has made clear that even multiple contacts with a forum state cannot give rise to general jurisdiction unless they "render [a defendant] essentially at home in the forum State"—which, for corporations, is typically limited to "the place of incorporation and principal place of business." *Daimler AG v. Bauman*, 134 S. Ct. 746, 760-61 (2014). Plaintiffs do not claim that any healthcare defendant is incorporated or principally conducts business in California; in fact, their complaint does not allege general jurisdiction at all.

In arguing for specific jurisdiction, plaintiffs artfully assert that the healthcare defendants "sen[t] users' sensitive medical communications to Facebook." PB 12. But that assertion is belied by plaintiffs' allegation that the URLs in question were transmitted *by their own browsers*. *See* p. 16 *infra*; Compl. ¶ 35. Moreover, plaintiffs do not allege that the transmissions were sent to California; they allege that Facebook is *headquartered* in California, but make no allegations about the locations of the data center(s) where their browsers actually sent referer headers.

Even if those allegations had been made, there would be no basis to conclude that the healthcare defendants "direct[ed their] activities . . . to the forum" or "purposefully availed [themselves] of the privilege of conducting activities in the forum." *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004). To the contrary, plaintiffs admit that they lack any knowledge as to whether the healthcare defendants were aware that the transfer of information was even occurring. Compl. ¶ 105. Moreover, all of the healthcare defendants provide services outside of California, and the named plaintiffs who claim to have visited their websites did so from locations outside of California. *Id.* ¶¶ 6-8. Plaintiffs do not allege that the

healthcare defendants' use of Facebook's code was an attempt to generate California-based revenue, target California citizens as patients, or harm plaintiffs' reputations in California. California simply has no connection whatsoever to their claims except for the fact that Facebook happens to be headquartered here. That is not enough, as the Supreme Court has already made plain. *See Walden v. Fiore*, 134 S. Ct. 1115, 1122 (2014) (holding that the "'minimum contacts' analysis looks to the defendant's contacts with the forum state itself, not the defendant's contacts with persons who reside there"); *see also FireClean, LLC v. Tuohy*, 2016 WL 3952093, at *5-8 & n.12 (E.D. Va. Jul. 21, 2016) (no personal jurisdiction notwithstanding the transmission of content to servers in Virginia and the accessibility of content by Virginia users; Facebook code cannot provide a basis for personal jurisdiction given its ubiquity). Plaintiffs merely allege that the healthcare defendants used code that happened to be created by a California company. If that were enough, the doctrine of personal jurisdiction would be meaningless.[5]

**B. The Eleventh Amendment Bars Jurisdiction over MD Anderson.**

Plaintiffs suggest that MD Anderson is not immune from suit because the Supreme Court held that sovereign immunity does not bar *state* courts from exercising jurisdiction over a sister state. PB 13. That is a non-sequitur—the immunity applies because this case was brought in *federal* court. *See Nevada v. Hall*, 440 U.S. 410, 420 (1979) ("[T]he Eleventh Amendment places explicit limits on the powers of federal courts to entertain suits against a State.").

[5] Plaintiffs also argue that "pursuant to Facebook's Terms of Service, . . . the health care Defendants[] submit to this Court's personal jurisdiction for the purpose of litigating all claims related to Facebook." PB 13. But plaintiffs have not alleged that any healthcare defendant entered into a contract with Facebook. And even if it had, any forum-selection clause would be irrelevant to claims by *plaintiffs* against the healthcare defendants. *See Concrete Washout Sys., Inc. v. Terrell Moran, Inc.*, 2015 WL 815835, at *2 (E.D. Cal. Feb. 25, 2015) (forum-selection clauses do "not apply . . . where a non-party to a contract [here, the plaintiffs] bears no relation to the signatory [here, the healthcare defendants] at the time of the execution of the contract, because such a non-party could not have participated in the transaction") (distinguishing *Holland Am. Line, Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 456 (9th Cir. 2007)). ACS's forum-selection clause, on the other hand, does control plaintiffs' claims against ACS. *See* ACS, User Agreement-Jurisdiction, *available at* http://www.cancer.org/aboutus/acspolicies/user-agreement. The Court should take judicial notice of ACS's Terms and Conditions because they are part of the documents plead in the complaint. *See Chambers v. Time Warner, Inc.* 282 F.3d 147, 152 (2d Cir. 2002)

Plaintiffs argue next, citing *Seitz v. City of Elgin*, 719 F.3d 654 (7th Cir. 2013), that Congress abrogated Eleventh Amendment immunity for liability under the Wiretap Act because the term "entity" in 18 U.S.C. § 2520 includes states. PB 13-14. But as *Seitz* itself recognized, Section 2520 "creates no substantive rights"; [i]t simply provides a cause of action to vindicate rights identified in *other portions* of the [Act]." 719 F.3d at 657 (emphasis added). The provision of the Wiretap Act at issue here applies only to "any person," not an "entity." 18 U.S.C. § 2511(1). Thus, Congress did not abrogate Eleventh Amendment immunity with respect to plaintiffs' claims in this case. *Seitz*, 719 F.3d at 660 ("[I]f we subject governmental units to suit for violations of § 2511(1), we ignore the statute's use of 'person' rather than 'person or entity.'"); *see also Hoffman v. Conn. Dep't of Income Maintenance*, 492 U.S. 96, 101 (1989) ("Congress must make its intention 'unmistakably clear' in the language of the statute").

## III. THE COMPLAINT SHOULD BE DISMISSED AS TO ALL DEFENDANTS UNDER RULE 12(b)(6).

### A. Plaintiffs' Claims All Fail Because They Consented to the Conduct at Issue.

Defendants argued that all of plaintiffs' claims are barred by their express allegation that they reviewed and consented to Facebook's Data Policy and Cookie Policy. DB 5-6, 16-18. In response, plaintiffs mischaracterize both the law and the relevant disclosures.

As a threshold matter: Plaintiffs argue that because consent is an "affirmative defense" and "consent does not appear in the Complaint, it should not be resolved on [a] 12(b)(6) motion." PB 14. That argument fails. First, the absence of consent is either an express or implicit *element* of each of plaintiffs' claims (*see* DB 16 & n.8); plaintiffs simply ignore the authorities that defendants cited. Second, the issue of consent "appears" *all over* the complaint; plaintiffs allege both that they are bound by Facebook's terms *and* that those terms do not encompass the conduct at issue here. *See, e.g.*, Compl. ¶¶ 3, 36, 39, 50(f), 52, 59, 225, 231, 266, 311, 326, 341, 347, 355; Exs. A-J (attaching defendants' terms of service). Courts have not hesitated to dismiss similar claims where, as here, the plaintiff's consent was directly implicated by the complaint and apparent from its face or its attachments. DB 17 (discussing *Perkins*, *Del Vecchio*, and *Mortensen*); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1029-30 (N.D. Cal. 2014).

**1. HIPAA and Its Consent Regime Do Not Apply.**

Plaintiffs argue that because this case allegedly implicates "sensitive medical information," HIPAA applies, and therefore they could consent to the disclosure of their information only through an express written authorization that complies with the statute. PB 14. But as defendants showed in the opening brief, HIPAA does not apply here as a matter of law for four reasons: (a) visiting a public web page is not a financial or administrative "*transaction*" regulated under HIPAA; (b) the URLs allegedly disclosed are not "*protected health information*" as defined by HIPAA; (c) because HIPAA provides *no private right of action*, the Court need not even address its specific provisions; and (d) plaintiffs concede that four of the defendants are not "*covered entities*" under the statute, meaning that HIPAA's requirements cannot possibly govern communications with those entities. DB 28-29.[6]

***No covered transaction.*** Visiting a public website is not a "transaction" under HIPAA. DB 28-29. Plaintiffs do not contend that it is, but argue that HIPAA is not limited to such transactions. PB 15. They are wrong. The Court "must give every word in a statute meaning." *Twentieth Century Fox Film Corp. v. Entm't Distrib.*, 429 F.3d 869, 885 (9th Cir. 2005). Congress repeatedly used the words "financial and administrative transactions" to define the scope of HIPAA. 42 U.S.C. § 1320d-2(a)(1), (2). These transactions include things like "[h]ealth claims," "[e]ligibility for a health plan," "payment and remittance advice," "premium payments," and "[e]lectronic funds transfers." *Id.* § 1320d-2(a)(2). Visiting a public website is not on the list, and plaintiffs have no authority suggesting it is covered by HIPAA.[7] *See also* 64

[6] Plaintiffs also briefly make a similar argument about California Civil Code § 1798.91. *See* PB 14, 17. Defendants' opening brief demonstrated that Section 1798.91 is inapplicable because it provides only that "[a] business may not *request in writing* medical information *directly from an individual*," Cal. Civ. Code § 1798.91(c) (emphases added), and because, like HIPAA, the statute does not provide a private right of action. DB 29. Plaintiffs do not respond, and many of the arguments on HIPAA set forth below apply similarly to the California statute.

[7] Plaintiffs only point to provisions of HIPAA that relate to obligations imposed (a) on a *covered* entity (b) *after* it has obtained *individually identifiable health information* (c) in the context of a *covered transaction*. PB 15 (citing 42 U.S.C. § 1320d-6(a)). Although these provisions do not repeat the covered transactions specified in HIPAA, they are all predicated on the existence of such a transaction. *See* 42 U.S.C. § 1320d-2(a)(1), (2).

Fed. Reg. 59918, 59918 (Nov. 3, 1999) ("This rule proposes standards to protect the privacy of individually identifiable health information *maintained or transmitted in connection with certain administrative and financial transactions*." (emphasis added)).

***No protected health information.*** Even assuming that HIPAA applied, plaintiffs have not alleged disclosure of the kind of *information* that it protects. HIPAA's governing regulations apply only to "*protected health information*," 45 C.F.R. § 164.502 (emphasis added), defined as "*individually identifiable information*" "created or received by a health care provider," *id.* § 160.103 (emphasis added). Information can be "individually identifiable" only if it "relates to the past, present, or future *physical or mental health* or condition of an *individual*," meaning the "*person* who is the subject of the protected health information." *Id.* (emphases added); *see also* DB 29. The complaint alleges no facts to support the conclusion that the information supposedly disclosed to Facebook is personally identifiable, sensitive, or related to plaintiffs' health. The communications alleged are limited to URLs that do not reveal plaintiffs' individual identities or relate these identities to any particular medical condition—they are static reference points. *See* DB Ex. A. Plaintiffs do not—and cannot—claim that their names, birthdates, billing information, or medical records were disclosed. In fact, plaintiffs do not allege even that they have the medical conditions referenced in the URLs (to the extent the URLs even identify a medical condition).[8] Nor do they allege that they were searching for information relating to treatment of their own condition, as opposed to general research or curiosity. Plaintiffs instead rely on HIPAA's "de-identification" regulation (PB 16 (citing 45 C.F.R. § 164.514(b)(2)), which does not purport to define the scope of "protected health information"; it only provides the process for de-identifying *already* protected health information so it can be shared.[9]

[8] With respect to BJC and Cleveland Clinic, plaintiff Jane Doe II concedes that the URLs at issue neither relate to her nor contain any identifying information about her; she claims to have visited the URLs not on her own behalf but on behalf of her spouse. PB 16.

[9] *See* Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, at 6 (2012), *available at* http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

***No private right of action.*** In any event, the Court need not address the specific provisions of HIPAA at all, because "HIPAA [ ] does not provide for a private right of action." *Webb*, 499 F.3d at 1082. If a plaintiff could import HIPAA's consent requirements into *other* causes of action—thereby *effectively* bringing a suit under HIPAA—"[t]he absence of a private right of action . . . would be rendered meaningless." *Astra USA, Inc. v. Santa Clara Cnty.*, 563 U.S. 110, 117-18 (2011); *see id.* at 114 (because plaintiffs "may not sue under [a] statute" providing no private right of action, "it would make scant sense to allow them to sue on a form contract implementing the statute, setting out terms identical to those contained in the statute"); *see also Cuyler v. United States*, 362 F.3d 949, 952 (7th Cir. 2004) (it is "clearly not the law" that "every statute that specified a standard of care [is] automatically enforceable by tort suits for damages"—that "every statute in effect would create a private right of action"). Plaintiffs point to no case in which a court has relied on HIPAA to supply the consent standard governing a separate statutory or common-law claim; to the contrary, courts routinely decline to incorporate HIPAA's provisions into other causes of action. *See Miller v. Elam*, 2011 WL 1549398, at *4 (E.D. Cal. Apr. 21, 2011) ("Because there is no private right of action under HIPAA, [a] HIPAA claim is not cognizable under 42 U.S.C. § 1983."); *Reed v. Columbia St. Mary's Hosp.*, 2014 WL 805919, at *3 (E.D. Wis. Feb. 28, 2014) ("invasion of privacy claim" based on allegation that "the defendant violated [HIPAA] by disclosing medical information without her consent . . . would [ ] fail"; "HIPAA does not furnish a private right of action").

***Not covered entities.*** Finally, as plaintiffs concede, only four of the defendants are covered entities under the statute: Adventist, BJC, Cleveland Clinic, and MD Anderson. Compl. ¶ 214; PB 15. It is therefore inconceivable that HIPAA's requirements could subject Facebook, ACS, ASCO, or MRF to any liability here. And it is equally inconceivable that HIPAA could determine whether *Facebook's* terms of service were adequate to obtain consent from plaintiffs. *See* DB16. Given their acknowledgement that Facebook, ACS, ASCO, and MRF had no duty whatsoever to comply with HIPAA, plaintiffs cannot credibly argue that HIPAA should govern alleged communications among those entities (*see* Compl. ¶¶ 117, 132, 147), or that Facebook's extensive disclosures should be viewed through HIPAA's lens (*see id.* ¶¶ 62, 71, 74).

**2. Facebook's Disclosures Were More Than Adequate.**

Ultimately, plaintiffs argue that they did not consent "even under Defendants' test" (*i.e.*, the test established by the case law): whether "a reasonable user who viewed [Facebook's] disclosures [would] have understood that [Facebook] was collecting [the information at issue]." PB 18 (quoting *Perkins*, 53 F. Supp. 3d at 1212). Plaintiffs make three main points; each fails.

First, plaintiffs contend that Facebook's disclosures were "buried in a privacy policy that no normal person ever reads (much less understands)." PB 2; *see* PB 18. That is contradicted by the complaint, which alleges that the SRR, Data Policy, and Cookie Policy "*constitute[] a valid contract*." Compl. ¶ 59 (emphasis added). Plaintiffs allege that "Facebook requires users to click a green Sign Up button" directly underneath text stating: "'By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.'" *Id.* ¶ 58. They do not allege that they failed to read, see, or understand these policies.[10] To the contrary, their fraud claim alleges that they *relied* on Facebook's policies to their detriment. *See id.* ¶ 366.

Second, plaintiffs say that Facebook's Data Policy and Cookie Policy are "vague." PB 2, 19. This assertion, too, is absent from the complaint. And even plaintiffs' brief fails to quote or identify a single "vague" aspect of the disclosures, presumably because Facebook could not have been clearer: It "collect[s] . . . information about the websites . . . you visit" with Facebook features from "all across the Internet and mobile ecosystem"; "use[s] all of the information we have about you to show you relevant ads"; and provides "third parties . . . with information about the reach and effectiveness of their advertising." DB 5-6, 16-17.[11]

---

[10] Any such allegation would be legally irrelevant: "[O]ne who signs a contract is bound by its provisions and cannot complain of unfamiliarity with the language of the instrument." *Circuit City Stores, Inc. v. Ahmed*, 283 F.3d 1198, 1200 (9th Cir. 2002).

[11] Plaintiffs quote the SRR's statements that "[y]our privacy is very important to us," and that "[w]e designed our Data Policy to make important disclosures about how you can use Facebook to share with others and how we collect and can use your content and information." PB 19 (quoting Compl. Ex A at 1). Plaintiffs make much of the "important disclosures" language (PB 4, 19), but that language merely directs users to the Data Policy: "By using Facebook Services, you agree that we can collect and use such content and information in accordance with the Data Policy" (Compl. Ex. A at 1, 3).

Third, plaintiffs contend that Facebook's disclosures "cannot be said to apprise reasonable persons that Facebook would track their sensitive medical communications with websites that explicitly promise not to make such disclosures." PB 19. This circular argument depends on the faulty assumptions (1) that the URLs at issue are "sensitive medical communications" (*but see* p. 11 *supra*) and (2) that the data tracking at issue was inconsistent with the healthcare defendants' policies (*but see* p. 15 *infra*). It is also nonsensical—plaintiffs appear to be suggesting that Facebook was required not only to list every conceivable form of arguably "sensitive" information that it might collect from third-party websites, but also to make disclosures about the adherence of the *third parties* to *their* policies.

There is no authority for these assertions. To the contrary: A contract term is not incomplete "just because it is broad," *F.B.T. Prods.*, 621 F.3d at 964, and disclosures about data collection cannot be "slice[d] . . . too thin," *Perkins*, 53 F. Supp. 3d at 1212. Accordingly, courts have bound plaintiffs to terms far more general than Facebook's. DB 17-18. In *Perkins*, Judge Koh held that LinkedIn could harvest email addresses from the plaintiffs' contact lists for marketing purposes by disclosing that LinkedIn was "asking for some information from" the email account. 53 F. Supp. 3d at 1212. *Del Vecchio* dismissed a claim about the cookie-tracking of sensitive financial information and mailing addresses because Amazon told users simply that it would "place . . . cookies on their computers and use those cookies to monitor and collect information." 2012 WL 1997697, at *6. And in *Mortensen*, the court held that the defendant was entitled to "funnel [its] customers' complete, unfiltered Internet traffic to a third-party processor for profiling and ad-serving" because it told customers that their "electronic transmissions would be monitored" and "transferred to third-parties for the purposes of providing 'content or services.'" 2010 WL 5140454, at *4-5. Facebook disclosed much more here.[12]

[12] *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003), is of no help to plaintiffs. *Cf.* PB 17-18. The pharmaceutical companies in that case "explicitly conditioned their purchase of [the defendant's product] on the fact that it would *not* collect [the] information" at issue. 329 F.3d at 20. Here, Facebook informed users that it would collect and use *all* of the information that could be derived from their browsing.

### 3. The Healthcare Defendants' Policies Were Likewise Adequate.

Although Facebook's disclosures were independently sufficient to put plaintiffs on notice of the conduct alleged in their complaint—barring all of their claims as to all of the defendants—the healthcare defendants' policies provided additional notice of the alleged conduct. DB 7-8, 18.[13] While the healthcare defendants' policies vary in the language used to notify users of their websites' policies and operations (because their business practices themselves vary), none promises that the referer headers at issue in this case would never be disclosed to third parties, and many state expressly that they *would* be disclosed. ASCO's policy, for example, notifies users of the precise conduct at issue in the complaint, stating that "the providers of third party Cookies may have the ability to link your activities on the Website with your browsing activities elsewhere on the Internet." Compl. Ex. G; *see also, e.g.*, Compl. Ex. F (ACS stating that general "traffic" information, such as a user's "browser information and length of stay" on a website, may be disclosed); Ex. H (MRF advising that "the date and time of [a user's] visit and the solutions and information for which [she] searched and which [she] viewed" may be disclosed); Exs. I, K (AHS and Cleveland Clinic disclosing that user IP addresses would be automatically collected and shared, and could be used to determine "a visitor's Internet Service Provider and the geographic location of his or her point of connectivity"); *id.* Ex. J (BJC disavowing confidentiality of web traffic information and noting use of third-party cookies to serve ads "based on [a user's] visit to [its] site").

## B. The Complaint Fails to Allege the Specific Elements of Each Claim.

### 1. Plaintiffs Fail to State a Claim under the Wiretap Act.

Plaintiffs failed to satisfy any of the three elements of their Wiretap Act claim: (a) an intentional interception (b) of content (c) using a device. DB 18-22.

[13] Plaintiffs argue that "the health care Defendants explicitly promise not to disclose [personally identifiable information ('PII')] to third-parties," and "[n]o reasonable person could read the health care Defendants' privacy promises and conclude that they disclose sensitive medical PII to Facebook in real-time." PB 3-5. Those promises have no bearing on this case, which alleges the disclosure of referer headers on public web pages—not PII. *See* p. 11 *supra*.

***Intentional interception***. Plaintiffs do not respond to defendants' argument that the Wiretap Act claim fails as to the healthcare defendants because the complaint disclaims any knowledge of whether they acted willfully. *See* DB 18 n.9, 22 n.12, 26 n.18; Compl. ¶ 5. The claim against the healthcare defendants must be dismissed on this basis alone.

Moreover, because each defendant was a party to all of the communications that it received from plaintiffs' browsers, none of those communications was "intercepted" and plaintiffs were never "wiretapped." DB 18-20. Plaintiffs recognize that their browsers sent two *separate* communications: (1) a GET request to the healthcare site asking that information be displayed on the browser; and (2) a separate GET request to Facebook accompanied by a referer header with the URL of the webpage on which Facebook content was being loaded. *See, e.g.*, PB 4-5. This concession dooms their claim: Facebook had no interaction with the first communication, and the healthcare defendants did not interact with the second. DB 19.

Plaintiffs do not dispute that the healthcare defendants were "parties" to the communications they received for purposes of the Wiretap Act. As to Facebook, they offer two responses, both of which are meritless. First, they cite *In re Pharmatrak*, 329 F.3d 9, 22 (1st Cir. 2003), for the proposition that a party can "intercept" a browser's communication if it receives a "[s]eparate, but simultaneous and identical, communication" from the browser. PB 20. But *Pharmatrak* did not address the Wiretap Act's "party" exception—§ 2511(2)(d)—because that exception was not before the court. More broadly, *Pharmatrak*'s discussion of the Wiretap Act's definition of "interception" cannot be squared with binding Ninth Circuit precedent holding that an electronic communication can be "intercepted" only if it is "*acquired during transmission*"—if it is "stop[ped], seize[d], or interrupt[ed] in progress or course." *Konop*, 302 F.3d at 878 (emphasis added). The transmission of a separate communication to a different recipient does not "stop, seize, or interrupt" the original communication; courts in this Circuit have thus followed *Konop* to hold that the simultaneous forwarding of exact copies of emails is not an "interception." *See Bunnell*, 567 F. Supp. 2d at 1153; *Crowley*, 166 F. Supp. 2d at 1269. By contrast, *Pharmatrak*'s discussion of the Act's "interception" requirement has never been mentioned in any case outside the First Circuit.

Second, plaintiffs argue that they "did not know Facebook was acquiring the communications they were exchanging with the health care Defendants." PB 21. But any lack of knowledge is irrelevant to the Wiretap Act: Because defendants "acquired the plaintiffs' Internet history information by way of GET requests that the plaintiffs sent directly to the defendants," they "have done nothing unlawful under the Wiretap Act." *Google Cookie Placement*, 806 F.3d at 142-43 (rejecting argument that a "deceit upon the sender" defeats the party exception to the Wiretap Act); *accord Nickelodeon*, 2016 WL 3513782, at *8-9; *see also* DB 20. Plaintiffs respond, bizarrely, that defendants' reliance on these authorities is "misplaced" because, "in the five months between those cases, the Third Circuit adopted a different rule, defining 'party to the communications' as 'an individual . . . whose participation in th[e] communication is known to the other participant(s) in the communication at the time of the communication.'" PB 21 (quoting *United States v. Eady*, __ F. App'x __, 2016 WL 2343212 (3d Cir. May 4, 2016)). *Eady* was a criminal case about a person's recordings of phone calls among other people, *see* 2016 WL 2343212, at *1; it does not apply to communications between computers (browsers and servers) whose "presence" cannot be "known" to one another. Moreover, *Eady* is unpublished; its analysis plainly cannot trump published opinions. And it did not purport to do so; *Eady* cited *Google Cookie Placement* with approval. *See id.* at *3.[14]

***Content***. Defendants argued that the URLs sent to Facebook by plaintiffs' browsers are not "content" under the Wiretap Act because they are just "record information regarding the characteristics of the message that is generated in the course of the communication." *Facebook Internet*, 140 F. Supp. 3d at 935 (quoting *Zynga*, 750 F.3d at 1106-07); DB 20-21. Plaintiffs

[14] Plaintiffs halfheartedly note that even if defendants fit within the "party" exception to the statute, they "may be liable" under the exception to that exception for circumstances in which a "'communication is intercepted for the purpose of committing any criminal or tortious act in violation of . . . the laws of the United States or of any State.'" PB 24 (quoting 18 U.S.C. § 2511(2)(d)). But they acknowledge that this exception applies only "where the underlying act is criminal or tortious for reasons unrelated to the means by which it was carried out." PB 24. There is "no legal authority providing that [this provision] is triggered when . . . the tortious conduct is the alleged wiretapping itself." *Google Cookie Placement*, 806 F.3d at 145. Plaintiffs pleaded no "facts to support an inference that [defendants] intercepted the communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording." *Id.*

respond that *Zynga* "explained that URLs contain content where they include 'search term[s] or similar communication[s] made by the user.'" PB 22 (quoting *Zynga*, 750 F.3d at 1109). *Zynga* did say in dicta that "[u]nder *some* circumstances, a user's request to a search engine for specific information could constitute . . . the contents of a communication. 750 F.3d at 1108-09 (emphasis added). But the court did not identify those circumstances, and it emphasized that a referer header would not be content even if it disclosed that a person viewed the "page of a gay support group." *Id.* at 1108. Plaintiffs fail to explain why the URLs alleged in the complaint are governed by *Zynga*'s dicta rather than its holding: that, in general, a URL does not convey the "meaning" of the communication with the host server but only the *location* of a webpage on the Internet. DB 21. The Court should follow *Zynga*'s holding and *Facebook Internet*.

***Device***. Plaintiffs invoke "[t]he dictionary definition of device." PB 23 (quoting definition on Dictionary.com). But the dictionary definition must yield to the *statutory* definition, which includes only items that "*can be used to intercept* a wire, oral, or electronic communication." 18 U.S.C. § 2510(5) (emphasis added). Plaintiffs still have not explained how the items listed in the complaint—such as a cookie, computer code, and Facebook's "plan"—could "intercept" a communication, or how Facebook *did* use them in this manner. DB 21.[15]

**2. Plaintiffs Fail to State a Claim under CIPA.**

***Section 631(a)***. Plaintiffs' claim under Section 631(a) of CIPA fails for the same basic reasons as their Wiretap Act claim:[16] (a) each defendant was a party to the communications it received; (b) those communications are not content; and (c) plaintiffs do not allege that Facebook acquired their communications using "a machine, instrument, or contrivance." DB 22-23; *see Facebook Internet*, 140 F. Supp. 3d at 936-37 (dismissing similar claim for second and third reasons). After "restat[ing]" their arguments on the Wiretap Act claim, which are addressed

[15] *In re Carrier IQ* (cited at PB 23) did not consider whether software is a "device." *See* 78 F. Supp. 3d at 1067. And the Seventh Circuit's decision in *Szymuszkiewicz* is inconsistent with this Circuit's precedents. *See* DB 21.

[16] As with the Wiretap Act claim, plaintiffs offer no response to defendants' argument that their CIPA claim fails against the healthcare defendants because the complaint disclaims any knowledge of whether they acted willfully. The CIPA claim also must be dismissed against the healthcare defendants on this basis alone. *See* Cal. Pen. Code § 631(a).

above, plaintiffs assert that CIPA "does not require a 'device' but instead prohibits interceptions 'by means of any machine, instrument, or contrivance, *or in any other manner*." PB 25 (quoting Cal. Penal Code § 631(a)). But "[w]here general words [in a statute] follow the enumeration of specific classes of things, the general words must be restricted to things of the same type as those specifically enumerated." *Aqua-Marine Constructors, Inc. v. Banks*, 110 F.3d 663, 677 (9th Cir. 1997). Thus, the phrase "in any other manner" must mean something *akin* to a "machine, instrument, or contrivance." Plaintiffs do not allege any such mechanism.

***Section 632(a)***. Plaintiffs failed to state a claim under Section 632(a) because they did not adequately allege (a) that the communications at issue were recorded by Facebook "without the[ir] consent"; (b) that they were "confidential"; or (c) that Facebook obtained them using an "electronic amplifying or recording device." DB 23. Plaintiffs' arguments on consent are addressed above. *See* Part III.A *supra*. As to confidentiality, they concede that "California courts have held that Internet communications cannot be considered confidential in some circumstances," but argue that "no California court has held that an Internet communication is not confidential when one of the parties to the communication explicitly promises that it will not be disclosed to a third-party," and that "the health care Defendants" made such a promise. PB 25. The healthcare defendants made no such promise (*see* p. 15 *supra*), and it would make no difference if they had: "Decisions from the California appellate courts . . . suggest that internet-based communications *cannot* be confidential" under CIPA. *Google Gmail*, 2013 WL 5423918, at *22 (emphasis added). On the third point, plaintiffs offer nothing but the assertion that defendants' argument "flies in the face of California courts' consistent modernizing of CIPA." PB 25. They do not address the "device" requirement in substance, and the cases that defendants cited were decided long after the Internet began. *See* DB 21.

***Preemption***. Defendants argued that plaintiffs' CIPA claim—along with all of their other state-law claims—is both expressly and impliedly preempted by the Wiretap Act. DB 24. Plaintiffs do not address express preemption. On implied preemption, plaintiffs regurgitate the reasoning of the cases that defendants acknowledged to be on one side of a split in authority. *See* PB 26; DB 24 n.16. Plaintiffs disregard the fundamental flaw in those cases: that a patchwork of

conflicting state causes of action would undermine the careful balance struck by Congress between privacy rights and free access to communications technologies, *see Google Street View*, 794 F. Supp. 2d at 1085—an objective whose importance is illustrated here. *See* DB 24.

***Extra-territoriality***. Defendants argued that plaintiffs cannot assert their CIPA claim—or their other state-law claims—against the healthcare defendants because they are not located in California. DB 25. Plaintiffs effectively concede the point, responding only that "Facebook's activities" occurred in California and that the healthcare defendants entered into a forum-selection clause with Facebook. PB 27. Facebook's forum-selection clause neither is alleged in the complaint nor plausibly supports extraterritorial application of California state law over the healthcare defendants. *See* n.5 *supra.* Plaintiffs cite no authority to suggest that it does.

**3. Plaintiffs Fail to State a Claim for Intrusion Upon Seclusion or California Constitutional Invasion of Privacy.**

***Intent***. As with their Wiretap Act and CIPA claims, plaintiffs' intrusion upon seclusion and California constitutional claims must be dismissed against the healthcare defendants for the sole reason that the complaint disclaims any knowledge of whether the healthcare defendants acted with intent—an element of the claims. *See* DB 26 n.18; *Schulman*, 18 Cal. 4th at 231.

***Reasonable expectation of privacy***. Plaintiffs have not alleged a reasonable expectation of privacy both because (a) courts have held that Internet users lack a reasonable expectation of privacy in the specific locations of websites they visit; and (b) plaintiffs failed to take the available measures to safeguard their information, including by opting out of targeted advertising. DB 26 (quoting *Facebook Internet*, 140 F. Supp. 3d at 933 n.5). Plaintiffs argue that they "allege[d] objectively reasonable expectations of privacy based upon federal and state statutes, as well as the explicit promises made by the health care Defendants with which [plaintiffs] were communicating." PB 29.

That argument is non-responsive. The question posed by the complaint is whether plaintiffs could reasonably expect that the *location* of the websites they visited would not be disclosed to anyone other than the healthcare defendants. And as the Ninth Circuit has explained—in a case decided when each of the statutes invoked by plaintiffs was in place—*no*

individual has such an expectation, because everyone who uses the Internet "should know that [the location of the websites they visit] is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *Forrester*, 512 F.3d at 510.[17] Nor do the healthcare defendants' alleged promises help plaintiffs; as discussed above (at p. 15), none of those commitments can plausibly be read to apply to the URLs at issue here.

***Highly offensive manner***. Even if plaintiffs had alleged facts supporting a reasonable expectation of privacy, this claim would still fail because they cannot satisfy the "highly offensive" prong of the test. Defendants' conduct was motivated by "legitimate business reasons"—not the kinds of "socially repugnant . . . reasons" that might be deemed "highly offensive" under California law. *Hernandez*, 47 Cal. 4th at 286, 297; *see* DB 26-28 (discussing *Hernandez*, *Fogelstrom*, *Google Privacy Policy*, *iPhone*, and *Low*). Plaintiffs ignore the caselaw and again rely on naked assertions: that "Plaintiffs alleged serious invasions of privacy that constitute an egregious breach of social norms" (PB 28), and that "Congress and every state" have made a "'policy' decision" that defendants' conduct is offensive "through the passage of criminal and civil laws designed to protect communications and healthcare privacy" (PB 29). But the issue is not whether the law generally protects "communications and healthcare privacy" on the Internet; it is whether defendants' *specific conduct*—the transmission and receipt of routine referer headers—is "highly offensive." And courts in this Circuit have unanimously "refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms." *Google Privacy Policy*, 58 F. Supp. 3d at 985.

Plaintiffs' intrusion cases (PB 28) are inapposite. In *Google Cookie Placement*, the plaintiffs alleged that Google had "overrid[den] the plaintiffs' cookie blockers" while assuring users that they would be effective, which "raise[d] different issues than tracking or disclosure

[17] *See also United States v. Caira*, __ F.3d __, 2016 WL 4376472, at *3 (7th Cir. Aug. 17, 2016) (no reasonable expectation of privacy in IP address associated with defendant's home); *Four Navy Seals v. Associated Press*, 413 F. Supp. 2d 1136, 1147 (S.D. Cal. 2005) ("[T]here is no reasonable expectation of privacy in transmissions over the internet."); *Deering v. CenturyTel, Inc.*, 2011 WL 1842859, at *2 (D. Mont. May 16, 2011) (dismissing intrusion upon seclusion claim; "no reasonable expectation of privacy when a plaintiff has been notified that his Internet activity may be forwarded to a third party to target him with advertisements")

alone." 806 F.3d at 150. In *Nickelodeon*, the defendant allegedly collected personal, private information from children despite telling their parents, "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!" 2016 WL 3513782, at *21. The court held that these "duplicitous tactics" plausibly stated an intrusion claim against that defendant, *id.* at *25, but rejected such a claim against another defendant (Google) that (like Facebook) had "used third-party cookies . . . in the same way that it deploys cookies on myriad other[] websites," *id.* at *24.[18] In *Opperman v. Path*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014), the intrusion claim was based on the "surreptitious theft of personal contact information" from a cell phone. *Id.* at 1061. None of these courts suggested that the mere transmission of a referer header could be highly offensive.

**4. Plaintiffs Have Not Asserted a Claim for "Negligence Per Se"**

Plaintiffs' so-called "negligence per se" claim fails because it does not exist as a separate cause of action, and because plaintiffs failed to allege the elements of a negligence claim. DB 28-30. Plaintiffs again fail to respond and simply repeat the allegation that "Defendants' conduct violated HIPAA" (PB 30)—a statute that is categorically inapplicable and could not support a negligence per se "claim" even if it applied. *See* DB 28-30; Part III.A.1 *supra*. They also argue that "Defendants' violation of [HIPAA] proximately caused Plaintiffs' injury." PB 30. That misstates the causation inquiry and finds no support in the complaint.

**5. Plaintiffs Fail to State a Claim Against the Healthcare Defendants for Negligent Disclosure of Confidential Information.**

Plaintiffs' claim against the healthcare defendants for negligent disclosure (*see* PB 30-31) must be dismissed because plaintiffs allege neither a duty to refrain from disclosing the URLs at issue nor any injury resulting from their alleged disclosure (*see* DB 30-32).

[18] Any broader reading of *Google Cookie Placement* would be inconsistent with California law and the Ninth Circuit's decision in *Forrester* (discussed above). Indeed, in *Nickelodeon*, which applied New Jersey privacy law, the court recognized that cases in the Ninth Circuit "suggest that a violation of a technology company's privacy-related terms of service is not offensive enough to make out a claim for invasion of privacy." 2016 WL 3513782, at *25 (citing *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013), which relied on California precedent to conclude that disclosing personal information in violation of a music streaming company's terms of service was not highly offensive).

***Duty***. Plaintiffs argue that the healthcare defendants undertook a duty when they "explicitly promised" not to disclose plaintiffs' "PII." PB 30. But they again fail to identify any particular promise that could reasonably apply to the allegedly disclosed URLs. The URLs are not, as plaintiffs contend, "sufficient to identify the visitor" or "pertinent to [the visitor's] health condition" (PB 31); they do not reveal plaintiffs' identities, and certainly do not reveal anyone's medical conditions or treatments. *See* p. 11 *supra*; DB Ex. A. To the contrary, they consist of the very information that the healthcare defendants' policies noted may be disclosed to third parties. *See* p. 15 *supra*; *see also, e.g.*, Compl. Ex. H (disclosing use of third-party servers); *id.* Exs. G, J (disclosing use of third-party cookies). Plaintiffs also argue that the URLs are "content" under the Wiretap Act and therefore *must* be PII. PB 31. The premise is wrong (*see* pp. 17-18 *supra*) and the conclusion does not follow from it.

***Injury***. Plaintiffs once more invoke generalized claims about privacy rights. PB 31. But the mere assertion of an injury, absent facts, does not establish this element of the claim. *See Ladd v. Cnty. of San Mateo*, 12 Cal. 4th 913, 917-18 (1996); *see also* pp. 3-4 *supra*. Plaintiffs try to distinguish their claims from those asserted in *Sony Gaming* and *Regents* (cited at DB 31-32) on the ground that those cases "did not allege that the data at issue had been misused" (PB 31-32). But the claims here are even weaker—the plaintiffs in *Sony Gaming* and *Regents* alleged increased risk of misuse, whereas plaintiffs here have not.

**6. Plaintiffs Fail to State a Claim Against the Healthcare Defendants for Breach of the Fiduciary Duty of Confidentiality.**

Plaintiffs concede that their only claimed basis for a fiduciary duty is their own voluntary choice to visit the healthcare defendants' websites. *See* PB 33; Compl. ¶¶ 117, 161, 175. Their suggestion that a visitor forms a fiduciary relationship with a website simply by visiting it is implausible, regardless of what information is on that website. Plaintiffs' assertion that the healthcare defendants had "complete control over plaintiffs' information" (PB 33) fares no better, as they concede that they communicated affirmatively and voluntarily with defendants' websites. Nor does it matter that the healthcare defendants maintain "privacy policies" (*id.*); as explained, those policies did not promise to protect as private the public URLs at issue, and the

defendants alerted users that web traffic and addressing information may sometimes be shared with third parties. *See* pp. 15 *supra*. Finally, even if a public website could somehow assume a fiduciary duty to each person who clicked a link to find it, plaintiffs do not claim any harm as a result of any breach of that duty.

**7. Plaintiffs Fail to State a Claim for Breach of the Duty of Good Faith and Fair Dealing Against Facebook.**

Plaintiffs have not stated a claim based on the duty of good faith and fair dealing for two reasons. First, Facebook fully complied with its disclosures, and second, the claim is grounded solely in a breach of the underlying contracts and is therefore not separately cognizable. DB 32. Plaintiffs respond that they seek "different and independent" relief on this count (PB 34), but they do not identify any such relief. They also argue that "there is no companion contract cause of action in the Complaint" (*id.*), but the key point is the existence of a *contract*, not a contract *claim*: "[T]he implied covenant of good faith and fair dealing cannot impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement." *Rosenfeld v. JPMorgan Chase Bank*, 732 F. Supp. 2d 952, 968 (N.D. Cal. 2010).

**8. Plaintiffs Fail to State a Claim for Fraud Against Facebook.**

After arguing that Facebook's disclosures were too "buried" for users to see and too "vague" for them to understand (PB 2), plaintiffs assert a claim that *depends* on alleging "with particularity" that those users read, believed, and relied on Facebook's representations. As a threshold matter, plaintiffs fail to sufficiently allege that Facebook's disclosures were false or inadequate (DB 16-18; Part III.A.2 *supra*); the Court therefore need not address the other elements of the fraud claim. But in any event, the two-sentence allegation in the complaint—that Facebook "suppress[ed]" certain facts "with the intent to deceive its users," and that plaintiffs "relied on Facebook's false assertions in contracting with and using Facebook" (Compl. ¶ 366)—is wholly inadequate to plead an intent to induce action, reliance, and damages. DB 33.

Plaintiffs respond as follows: "Plaintiffs alleged intent to deceive, reliance, and damages arising [from Facebook's statements], which satisfies the elements [of fraud]." PB 34. In an action for fraud, there is a well-established need to "protect [defendants] from the harm that

comes from being subject to fraud charges" and "safeguard[ their] reputation and goodwill from improvident charges of wrongdoing." *Vess*, 317 F.3d at 1104. Plaintiffs may not bring such a claim and then leave Facebook and the Court guessing as to the facts (if any) showing that plaintiffs were defrauded. For all we know from plaintiffs' filings, no member of the purported class altered his behavior in the slightest as a result of Facebook's disclosures, let alone to his detriment. *See Engala*, 15 Cal. 4th at 976; *Moncada*, 221 Cal. App. 4th at 776.

**9. Plaintiffs Have No Claim Against Facebook for Quantum Meruit.**

Plaintiffs' final claim based on Facebook's alleged unjust enrichment (a) is not a standalone cause of action, (b) fails because of the existence of an enforceable agreement, and (c) does not show how Facebook obtained an "unjust benefit [that] was retained at plaintiffs' expense." DB 34. Plaintiffs are silent on each of these points; they merely insist that "Facebook cannot justly retain the benefit it obtained from violating Plaintiffs' privacy rights," and demand "compensation." PB 35 (citation omitted). This supposed claim, too, must be dismissed.

**CONCLUSION**

Like *Facebook Internet*, this case is based on the everyday collection and use of data for purposes of providing free Internet services that people want or need. That is why none of the plaintiffs can claim any harm from this conduct; why none can claim any unlawful purpose on the part of the defendants; and why the terms "privacy" and "medical information" are repeatedly invoked as talismans without explanation. There is no question that the privacy of Internet users is important. But defendants have done nothing to undermine that privacy. The Court should grant defendants' motion and dismiss this case with prejudice.

Dated: August 22, 2016

MAYER BROWN LLP

By: /s/ John Nadolenco
JOHN NADOLENCO, State Bar No. 181128
jnadolenco@mayerbrown.com
350 South Grand Avenue, 25th Floor
Los Angeles, California 90071-1503
Telephone: (213) 229-9500
Facsimile: (213) 625-0248

LAUREN R. GOLDMAN*
lrgoldman@mayerbrown.com
1221 Avenue of the Americas
New York, NY 10020-1001
Telephone: (212) 506-2500
Facsimile: (212) 262-1910

**Admitted pro hac vice*

*Attorneys for Defendant*
*FACEBOOK, INC.*

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Michael H. Rubin
MICHAEL H. RUBIN, State Bar No. 214636
mrubin@wsgr.com
PETER C. HOLM, State Bar No. 299233
pholm@wsgr.com
1 Market Street
Spear Tower, Suite 3300
San Francisco, CA 94105
Telephone: (415) 947-2000
Facsimile: (415) 947-2099

ANTHONY J WEIBELL, State Bar No. 238850
aweibell@wsgr.com
LAUREN GALLO WHITE, State Bar No. 309075
lwhite@wsgr.com
650 Page Mill Road
Palo Alto, CA 94304
Telephone: (650) 493-9300
Facsimile: (650) 565-5100

*Attorneys for Defendant*
*BJC HEALTHCARE*

HOLLAND & KNIGHT LLP

By: /s/Shelley G. Hurwitz
SHELLEY G. HURWITZ, State Bar No. 217566
400 S. Hope St., 8th Floor
Los Angeles, CA 90071
Telephone: (213) 896-2400
Facsimile: (213) 896-2450

JOHN P. KERN, State Bar No. 206001
DAVID I. HOLTZMAN, State Bar No. 299287
50 California Street, Suite 2800
San Francisco, CA 94111
Telephone: (415) 743-6900
Facsimile: (415) 743-6910

STEVEN B. ROOSA*
31 West 52 Street
New York, NY 10019
Telephone: (212) 513-3544
Facsimile: (212) 513-3544

*Attorneys for Defendants*
*ADVENTIST HEALTH SYSTEM SUNBELT HEALTHCARE CORPORATION (SUED AS "ADVENTIST HEALTH SYSTEM");*
*AMERICAN CANCER SOCIETY, INC.; AND*
*MELANOMA RESEARCH FOUNDATION*

**Pro hac vice application to be filed*

JONES DAY

By: /s/ Jeffrey Rabkin
JEFFREY RABKIN, State Bar No. 189798
jrabkin@jonesday.com
BRANDY H. RANJAN*
branjan@jonesday.com
ALEXANDRA A. MCDONALD, State Bar No. 300950
amcdonald@jonesday.com
555 California Street, 26th Floor
San Francisco, CA 94104
Telephone: (415) 875-5850
Facsimile: (415) 875-5700

* *Admitted pro hac vice*

BRIAN G. SELDEN, State Bar No. 261828
bgselden@jonesday.com
1755 Embarcadero Road
Palo Alto, CA 94303
Telephone: (650) 739-3939
Facsimile: (650) 739-3900

*Attorneys for Defendant*
*AMERICAN SOCIETY OF CLINICAL ONCOLOGY, INC.*

BAKER & HOSTETLER LLP

By: /s/ Teresa Chow
TERESA CHOW, State Bar No. 237694
tchow@bakerlaw.com
11601 Wilshire Boulevard, Suite 1400
Los Angeles, CA 90025-0509
Telephone: (310) 820-8800
Facsimile: (310) 820-8859

STEVEN M. DETTELBACH*
sdettelbach@bakerlaw.com
DANIEL R. WARREN*
dwarren@bakerlaw.com
DAVID A. CARNEY*
dcarney@bakerlaw.com
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

* *Admitted pro hac vice*

*Attorneys for Defendant*
*CLEVELAND CLINIC*

BAKER & HOSTETLER LLP

By: /s/ Teresa Chow
TERESA CHOW, State Bar No. 237694
tchow@bakerlaw.com
11601 Wilshire Boulevard, Suite 1400
Los Angeles, CA 90025-0509
Telephone: (310) 820-8800
Facsimile: (310) 820-8859

PAUL G. KARLSGODT*
pkarlsgodt@bakerlaw.com
CASIE COLLIGNON*
ccollignon@bakerlaw.com
1801 California Street, Suite 4400
Denver, CO 80202-2662
Telephone: (303) 861-0600
Facsimile: (303) 861-7805

* *Admitted pro hac vice*

*Attorneys for Defendant*
*UNIVERSITY OF TEXAS—MD*
*ANDERSON CANCER CENTER*

**ATTESTATION**

I, John Nadolenco, hereby attest, pursuant to N.D. Cal. Local Rule 5-1(i)(3), that concurrence to the filing of this document has been obtained from each signatory.

By: */s/ John Nadolenco*
John Nadolenco